FORTINET

# FortiOS™ Handbook - Logging and Reporting

VERSION 6.0.0

FORTIOS VERSION 6.0

**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**FORTICAST**

http://forticast.fortinet.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FORTINET PRIVACY POLICY**

https://www.fortinet.com/corporate/about-us/privacy.html

**FEEDBACK**

Email: techdocs@fortinet.com

March 29, 2018

FortiOS™ Handbook - Logging and Reporting

01-600-481081-20180329

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| March 29, 2018 | Official release for FortiOS 6.0. See "What's new in FortiOS 6.0" on page 9. |
| | |
| | |
| | |

# Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This document provides detailed information that explains how to take advantage of your FortiGate's ability to log and report activity, whether you need to monitor network stability, log traffic offsite for security reasons, provide bandwidth usage reports, or one of many other possible functions.

Logging is an integral component of the FortiGate system. Logging allows you to view the activity and status of the traffic passing through your network, and monitor for anomalies.

If you notice problems with this document, or have suggestions for improvements, send an email about them to Fortinet Technical Document at techdoc@fortinet.com.

## Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

### How this guide is organized

This document contains information about how to find the right log device for your logging requirements, how to enable and configure logging to that device, and a detailed explanation of each log type log message.

This FortiOS Handbook chapter contains the following sections:

Logging and reporting overview provides general information about logging. We recommend that you begin with this chapter as it contains information for both beginners and advanced users as well. It contains an explanation of log messages, files, and devices, and an overview of the Reporting functions.

Logging and reporting for small networks provides an overview of setting up a small network for logging, with a look at a possible setup with a backup solution and a customized report.

Logging and reporting for large networks provides an overview of setting up a larger, enterprise-level network, with configuration of multiple FortiGate units, multiple FortiAnalyzer units as a backup solution, and a sample procedure for creating a more intensive and broad report to suit the larger network.

Advanced logging provides a series of separate tutorials for possible tasks and procedures an advanced user may want to undertake with their FortiGate-powered network. It contains explanations of advanced backup, logging, and report solutions.

Troubleshooting and logging provides a short overview of how log messages can be used to identify and solve problems within the network, how to identify and solve logging database issues, and how to solve connection issues between FortiGate and FortiAnalyzer units.

# What's new in FortiOS 6.0

The following list contains new Logging & Reporting features added in FortiOS 6.0.

## Automatic synchronization of log display location

In previous versions, log display location could differ between Log & Report and FortiView, which could result in empty log screens if the two were not synchronized. Now, both log viewers automatically pick the best available log device. A different log device can be manually selected.

As a result, the associated CLI command `log gui-display location` has been removed.

## Improved log messages for SD-WAN link quality changes

FortiOS 6.0 introduces two new log messages:

- 22923: LOG_ID_EVENT_VWL_LQTY_STATUS is created when a member's link quality is changed.
- 22924: LOG_ID_EVENT_VWL_VOLUME_STATUS is used only when `load-balance-mode` is set to `measured-volume-based`. The log is created when a member starts or stops receiving traffic.

## Extended UTM logging and improved syslog configuration

Multiple UTM features now have the ability to enable extended logging: WAF, Web Filtering, DLP, AntiVirus.

These new features can be enabled in the CLI:

```
config waf profile
   edit <profile name>
      set extended-log {enable | disable}
      end
config webfilter profile
   edit <profile name>
      set web-extended-log {enable | disable}
      set web-extended-all-action-log {enable | disable}
      end
config dlp sensor
   edit <sensor name>
      set dlp-extended-log {enable | disable}
      end
config antivirus profile
   edit <profile name>
      set av-extended-log {enable | disable}
      end
```

## Updated reliable syslog encryption to comply with RFC 5425

In order to align with RFC 5425 (syslog on an encrypted TLS connection over TCP) and general logging security standards for syslog, reliable syslog encryption is customizable in the CLI:

```
config log syslog setting
   set enc-algorithm {high-medium | high | low | disable}
   end
```

Also, syslog options for reliable logging transmission have been expanded:

```
config log syslog setting
   set mode {udp | legacy-reliable | reliable}
   end
```

See the *FortiOS CLI Reference* for more information about these commands.

## Improved log display consistency at high load

Previous versions could display inconsistent log data when using Drill Down charts and when navigating between different log tables (in both **Log & Report** and **FortiView**). The maximum number of records now varies based on length that logs are kept, relative to device model size. Record numbers are configurable in `config report setting`.

Log database queries used to collect **Top Sources** and **Top Destinations** data are significantly more efficient due to improved indexing speed.

# Logging and reporting overview

Logging and reporting in FortiOS can help you in determining what is happening on your network, as well as informing you of certain network activity, such as detection of a virus or IPsec VPN tunnel errors. Logging and reporting go hand in hand, and can become a valuable tool for information as well as helping to show others the activity that is happening on the network.

This section explains logging and reporting features that are available in FortiOS, and how they can be used to help you manage or troubleshoot issues. This includes how the FortiGate unit records logs, what a log message is, and what the log database is.

## What is logging?

Logging records the traffic passing through the FortiGate unit to your network and what action the FortiGate unit took during its scanning process of the traffic. This recorded information is called a log message.

After a log message is recorded, it is stored within a log file which is then stored on a log device. A log device is a central storage location for log messages. The FortiGate unit supports several log devices, such as FortiAnalyzer units, the FortiCloud service, and Syslog servers. A FortiGate unit's system memory and local disk can also be configured to store logs, and because of this, are also considered log devices.

You must subscribe to FortiCloud before you will be able to configure the FortiGate unit to send logs to a FortiCloud server.

When the recorded activity needs to be read in a more human way, the FortiGate unit can generate a Report. A report gathers all the log information that is needed for the report, and presents it in a graphical format, with customizable design and automatically generated charts. Reports can be used to present a graphical representation of what is going on in the network. Reports can also be generated on a FortiAnalyzer unit; if you want to generate reports on a FortiAnalyzer, see the FortiAnalyzer Setup and Administration Guide to help you create and generate those reports.

### How the FortiGate unit records log messages

The FortiGate unit records log messages in a specific order, storing them on a log device. The order of how the FortiGate unit records log messages is as follows:

1. Incoming traffic is scanned.
2. During the scanning process, the FortiGate unit performs necessary actions, and simultaneously records the actions and results.
3. Log messages are sent to the log device.

#### Example: How the FortiGate unit records a DLP event

1. The FortiGate unit receives incoming traffic and scans for any matches associated within its firewall policies containing a DLP sensor.

2. A match is found; the DLP sensor, dlp_sensor, had a rule within it called All-HTTP with the action Exempt applied to the rule. The sensor also has Enable Logging selected, which indicates to the FortiGate unit that the activity should be recorded and placed in the DLP log file.
3. The FortiGate unit exempts the match, and places the recorded activity (the log message) within the DLP log file.
4. According to the log settings that were configured, logs are stored on the FortiGate unit's local hard drive. The FortiGate unit places the DLP log file on the local hard drive.

# FortiOS features available for logging

Logs record FortiGate activity, providing detailed information about what is happening on your network. This recorded activity is found in log files, which are stored on a log device. However, logging FortiGate activity requires configuring certain settings so that the FortiGate unit can record the activity. These settings are often referred to as log settings, and are found in most security profiles, but also in **Log & Report > Log Settings**.

Log settings provide the information that the FortiGate unit needs so that it knows what activities to record. This topic explains what activity each log file records, as well as additional information about the log file, which will help you determine what FortiGate activity the FortiGate unit should record.

## Traffic

Traffic logs record the traffic that is flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through the unit, this type of logging is also referred to as firewall policy logging. Firewall policies control all traffic that attempts to pass through the FortiGate unit, between FortiGate interfaces, zones and VLAN sub-interfaces.

Logging traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic)
- packet comes into an inbound interface
- a possible log packet is sent regarding a match in the firewall policy, such as a URL filter
- traffic log packet is sent, per firewall policy
- packet passes and is sent out an interface

Traffic log messages are stored in the traffic log file. Traffic logs can be stored any log device, even system memory.

All security profile-related logs are now tracked within the Traffic logs, as of FortiOS 5.0, so all forward traffic can be searched in one place, such as if you are looking to see all activity from a particular address, security feature or traffic. Security profile logs are still tracked separately in the **Security Log** section, which only appears when logs exist.

If you have enabled and configured WAN Optimization, you can enable logging of this activity in the CLI using the `config wanopt setting` command. These logs contain information about WAN Optimization activity and are found in the traffic log file. When configuring logging of this activity, you must also enable logging within the security policy itself, so that the activity is properly recorded.

## Sniffer

The Sniffer log records all traffic that passes through a particular interface that has been configured to act as a One-Armed Sniffer, so it can be examined separately from the rest of the Traffic logs.

## Other Traffic

The traffic log also records interface traffic logging, which is referred to as Other Traffic. Other Traffic is enabled only in the CLI. When enabled, the FortiGate unit records traffic activity on interfaces as well as firewall policies. Logging Other Traffic puts a significant system load on the FortiGate unit and should be used only when necessary.

Logging other traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic) and other-traffic
- packet comes into an interface
- interface log packet is sent to the traffic log that is enabled on that particular interface
- possible log packet is sent regarding a match in the firewall policy, such as URL filter
- interface log packet is sent to the traffic log if enabled on that particular interface
- packet passes and is sent out an interface
- interface log packet is sent to traffic (if enabled) on that particular interface

## Event

The event log records administration management as well as FortiGate system activity, such as when a configuration has changed, admin login, or high availability (HA) events occur. Event logs are an important log file to record because they record FortiGate system activity, which provides valuable information about how your FortiGate unit is performing.

Event logs help you in the following ways:

- keeping track of configuration setting changes
- IPsec negotiation, SSL VPN and tunnel activity
- quarantine events, such as banned users
- system performance
- HA events and alerts
- firewall authentication events
- wireless events on models with WiFi capabilities
- activities concerning modem and internet protocols L2TP, PPP and PPPoE
- VIP activities
- AMC disk's bypass mode
- VoIP activities that include SIP and SCCP protocols.

As of 5.4, every 'execute' CLI command now generates an 'audit' event log, allowing you to track configuration changes. You can enable/disable this feature in the CLI:

```
config system global
   set cli-audit-log [enable|disable]
end
```

The FortiGate unit records event logs only when events are enabled.

## Traffic Shaping

Traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings can be applied to a firewall policy, appearing within the traffic log messages.

By enabling this feature, you can see what traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings are being used.

## Data Leak Prevention

Data Leak Prevention logs, or DLP logs, provide valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network. The DLP rules within a DLP sensor can log the following traffic types:

- email (SMTP, POP3 or IMAP; if SSL content SMTPS, POP3S, and IMAPS)
- HTTP
- HTTPS
- FTP
- NNTP
- IM

A DLP sensor must have log settings enabled for each DLP rule and compound rule, as well as applied to a firewall policy so that the FortiGate unit records this type of activity. A DLP sensor can also contain archiving options, which these logs are then archived to the log device.

## NAC Quarantine

Within the DLP sensor, there is an option for enabling NAC Quarantine. The NAC Quarantine option allows the FortiGate unit to record details of DLP operation that involve the ban and quarantine actions, and sends these to the event log file. The NAC Quarantine option must also be enabled within the Event Log settings. When enabling NAC quarantine within a DLP Sensor, you must enable this in the CLI because it is a CLI-only command.

## Media Access Control (MAC) Address

MAC address logs provide information about MAC addresses that the FortiGate unit sees on the network as well as those removed from the network. These log messages are stored in the event log (as subtype network; you can view these log messages in **Log & Report > System Events**) and are, by default, disabled in the CLI. You can enable logging MAC addresses using the following command syntax:

```
config log setting
   set neighbor-event enable
end
```

When enabled, a new log message is recorded every time a MAC address entry is added to the ARP table, and also when a MAC address is removed as well. A MAC address log message is also recorded when MAC addresses are connected to the local switch, or from a FortiAP or FortiSwitch unit.

## Application control

Application control logs provide detailed information about the traffic that internet applications such as Skype are generating. The application control feature controls the flow of traffic from a specific application, and the FortiGate unit examines this traffic for signatures that the application generates.

The log messages that are recorded provide information such as the type of application being used (such as P2P software), and what type of action the FortiGate unit took. These log messages can also help you to determine the top ten applications that are being used on your network. This feature is called application control monitoring and you can view the information from a widget on the Executive Summary page.

The application control list that is used must have logging enabled within the list, as well as logging enabled within each application entry. Each application entry can also have packet logging enabled. Packet logging for application control records the packet when an application type is identified, similar to IPS packet logging.

Logging of application control activity can only be recorded when an application control list is applied to a firewall policy, regardless of whether or not logging is enabled within the application control list.

## Antivirus

Antivirus logs are recorded when, during the antivirus scanning process, the FortiGate unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature. Antivirus logs provide a way to understand what viruses are trying to get in, as well as additional information about the virus itself, without having to go to the FortiGuard Center and do a search for the detected virus. The link is provided within the log message itself.

These logs provide valuable information such as:

- the name of the detected virus
- the name of the oversized file or infected file
- the action the FortiGate unit took, for example, a file was blocked
- URL link to the FortiGuard Center which gives detailed information about the virus itself

The antivirus profile must have log settings enabled within it so that the FortiGate unit can record this activity, as well as having the antivirus profile applied to a firewall policy.

## Web Filter

Web filter logs record HTTP traffic activity. These log messages provide valuable and detailed information about this particular traffic activity on your network. Web filtering activity is important to log because it can inform you about:

- what types of web sites employees are accessing
- users attempting to access banned web sites and how often this occurs
- network congestion due to employees accessing the Internet at the same time
- web-based threats resulting from users visiting non-business-related web sites

Web Filter logs are an effective tool to help you determine if you need to update your web filtering settings within a web filter profile due to unforeseen threats or network congestion. These logs also inform you about web filtering quotas that have been configured for filtering HTTP traffic.

You must configure logging settings within the web filter profile and apply the filter to a firewall policy so that the FortiGate unit can record the activity.

## IPS (attack)

IPS logs, also referred to as attack logs, record attacks that occurred against your network. Attack logs contain detailed information about whether the FortiGate unit protected the network using anomaly-based defense settings or signature-based defense settings, as well as what the attack was.

The IPS or attack log file is especially useful because the log messages that are recorded contain a link to the FortiGuard Center, where you can find more information about the attack. This is similar to antivirus logs, where a link to the FortiGuard Center is provided as well that informs you of the virus that was detected by the FortiGate unit.

An IPS sensor with log settings enabled must be applied to a firewall policy so that the FortiGate unit can record the activity.

## Packet logs

When you enable packet logging within an IPS signature override or filter, the FortiGate unit examines network packets, and if a match is found, saves them to the attack log. Packet logging is designed to be used as a diagnostic tool that can focus on a narrow scope of diagnostics, rather than a log that informs you of what is occurring on your network.

You should use caution when enabling packet logging, especially within IPS filters. Filter configuration that contains thousands of signatures could potentially cause a flood of saved packets, which would take up a lot of storage space on the log device. It would also take a great deal of time to sort through all the log messages, as well as consume considerable system resources to process.

You can archive packets, but you must enable this option on the Log Settings page. If your log configuration includes multiple FortiAnalyzer units, packet logs are only sent to the primary (first) FortiAnalyzer unit. Sending packet logs to the other FortiAnalyzer units is not supported.

## Email filter

Email filter logs, also referred to as spam filter logs, record information regarding the content within email messages. For example, within an email filter profile, a match is found that finds the email message to be considered spam.

Email filter logs are recorded when the FortiGate unit finds a match within the email filter profile and logging settings are enabled within the profile.

If you are using a Banned Words List for email filtering, note that the filter pattern number is only recorded when the source email address contains a banned word.

## Archives (DLP)

Recording DLP logs for network use is called DLP archiving. The DLP engine examines email, FTP, IM, NNTP, and web traffic. Archived logs are usually saved for historical use and can be accessed at any time. IPS packet logs can also be archived, within the Log Settings page.

You can start with the two default DLP sensors that have been configured specifically for archiving log data, Content_Archive and Content_Summary. They are available in **Security Profiles > Data Leak Prevention**. Content_Archive provides full content archiving, while Content_Summary provides summary archiving. For more information about how to configure DLP sensors, see the Security Features chapter of the FortiOS Handbook.

You must enable the archiving to record log archives. Logs are not archived unless enabled, regardless of whether or not the DLP sensor for archiving is applied to the firewall policy.

### Network scan

Network scan logs are recorded when a scheduled scan of the network occurs. These log messages provide detailed information about the network's vulnerabilities regarding software, as well as the discovery of any further vulnerabilities.

A scheduled scan must be configured and logging enabled within the Event Log settings, for the FortiGate unit to record these log messages.

## Log messages

Log messages are recorded by the FortiGate unit, giving you detailed information about the network activity. Each log message has a unique number that helps identify it, as well as containing fields; these fields, often called log fields, organize the information so that it can be easily extracted for reports.

These log fields are organized in such a way that they form two groups: the first group, made up of the log fields that come first, is called the log header. The log header contains general information, such as the unique log identification and date and time that indicates when the activity was recorded. The log body is the second group, and contains all the other information about the activity. There are no two log message bodies that are alike, however, there may be fields common to most log bodies, such as the `srcintf` or `identidix` log fields.

The log header also contains information about the log priority level which is indicated in the `level` field. The priority level indicates the immediacy and the possible repercussions of the logged action. For example, if the field contains 'alert', you need to take immediate action with regards to what occurred. There are six log priority levels.

The log severity level is the level at and above which the FortiGate unit records logs. The log severity level is defined by you when configuring the logging location. The FortiGate unit will log all messages at and above the priority level you select. For example, if you select Error, the unit will log only Error, Critical, Alert, and Emergency level messages.

**Log priority levels**

| Levels | Description |
|---|---|
| **0 - Emergency** | The system has become unstable. |
| **1 - Alert** | Immediate action is required. |
| **2 - Critical** | Functionality is affected. |
| **3 - Error** | An error condition exists and functionality could be affected. |

| Levels | Description |
|---|---|
| **4 - Warning** | Functionality could be affected. |
| **5 - Notification** | Information about normal events. |
| **6 - Information** | General information about system operations. |

The Debug priority level, not shown above, is rarely used. It is the lowest log priority level and usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly.

### Example log header fields

| Log header | |
|---|---|
| **date=(2010-08-03)** | The year, month and day of when the event occurred in yyyy-mm-dd format. |
| **time=(12:55:06)** | The hour, minute and second of when the event occurred in the format hh:mm:ss. |
| **log_id=(2457752353)** | A five or ten-digit unique identification number. The number represents that log message and is unique to that log message. This ten-digit number helps to identify the log message. |
| **type=(dlp)** | The section of system where the event occurred. |
| **subtype=(dlp)** | The subtype category of the log message. |
| **level=(notice)** | The priority level of the event. See the table above. |
| **vd=(root)** | The name of the virtual domain where the action/event occurred in. If no virtual domains exist, this field always contains root. |

### Example log body fields

| Log body | |
|---|---|
| **policyid=(1)** | The ID number of the firewall policy that applies to the session or packet. Any policy that is automatically added by the FortiGate will have an index number of zero. |
| **identidx=(0)** | The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy. |
| **sessionid=(311)** | The serial number of the firewall session of which the event happened. |
| **srcip=(10.10.10.1)** | The source IP address. |

| Log body | |
|---|---|
| **srcport=(1190)** | The source port number. |
| **srcintf=(internal)** | The source interface name. |
| **dstip=(192.168.1.122)** | The destination IP address. |
| **dstport=(80)** | The destination port number. |
| **dstintf=(wan1)** | The destination interface name. |
| **service=(https)** | The IP network service that applies to the session or packet. The services displayed correspond to the services configured in the firewall policy. |
| **status=(detected)** | The action the FortiGate unit took. |
| **hostname=(example.com)** | The home page of the web site. |
| **url=(/image/trees_pine_ forest/)** | The URL address of the web page that the user was viewing. |
| **msg=(data leak detected (Data Leak Prevention Rule matched)** | Explains the FortiGate activity that was recorded. In this example, the data leak that was detected matched the rule, All-HTTP, in the DLP sensor. |
| **rulename=(All-HTTP)** | The name of the DLP rule within the DLP sensor. |
| **action=(log-only)** | The action that was specified within the rule. In some rules within sensors, you can specify content archiving. If no action type is specified, this field display log-only. |
| **severity=(1)** | The level of severity for that specific rule. |

Logs from other devices, such as the FortiAnalyzer unit and Syslog server, contain a slightly different log header. For example, when viewing FortiGate log messages on the FortiAnalyzer unit, the log header contains the following log fields when viewed in the Raw format:

```
itime=1302788921 date=20110401 time=09:04:23 devname=FG50BH3G09601792 device_
    id=FG50BH3G09601792 log_id=0100022901 type=event subtype=system level=notice vd=root
```

The log body contains the rest of the information of the log message, and this information is unique to the log message itself.

For detailed information on all log messages, see the *FortiGate Log Message Reference*.

## Explanation of a debug log message

Debug log messages are only generated if the log severity level is set to Debug. The Debug severity level is the lowest log severity level and is rarely used. This severity level usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly. Debug log messages are generated by all types of FortiGate features.

The following is an example of a debug log message:

```
date=2010-01-25 time=17:25:54 logid=9300000000 type=webfilter subtype=urlfilter
    level=debug msg="found in cache"
```

**Example of a Debug log message**

| Debug log | |
|---|---|
| **date=(2010-01-25)** | The year, month and day of when the event occurred in the format yyyy-mm-dd. |
| **time=(17:25:54)** | The hour, minute and second of when the event occurred in the format hh:mm:ss. |
| **logid=(93000000000)** | A ten-digit unique identification number. The number represents that log message and is unique to that log message. This ten-digit number helps to identify the log message. |
| **type=(webfilter)** | The section of system where the event occurred. There are eleven log types in FortiOS 4.0. |
| **subtype=(urlfilter)** | The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy. |
| **level=(debug)** | The priority level of the event. There are six priority levels to specify. |
| **msg=("found in cache")** | Explains the activity or event that the FortiGate unit recorded. |

## Viewing log messages and archives

Depending on the log device, you may be able to view logs within the web-based manager or CLI on the FortiGate unit. If you have configured a FortiAnalyzer unit, local hard disk, or system memory, you can view log messages from within the web-based manager or CLI. If you have configured either a Syslog or WebTrends server, you will not be able to view log messages from the web-based manager or CLI. There is also no support for viewing log messages stored on a FortiCloud server, from the FortiGate unit's web-based manager or CLI.

You do not have to view log messages from only the web-based manager. You can view log messages from the CLI as well, using the `execute log display` command. This command allows you to see specific log messages that you already configured within the `execute log filter` command. The `execute log filter` command configures what log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view. For more information about viewing log messages in the CLI, see "Viewing logs from the CLI".

There are two log viewing options in FortiOS: Format and Raw. The Raw format displays logs as they appear within the log file. You can view log messages in the Raw format using the CLI or a text editor, such as Notepad. Format is in a more human-readable format, and you can easily filter information when viewing log messages this way. The Format view is what you see when viewing logs in the web-based manager.

When you download the log messages from within the log message page (for example, **Log & Report > Forward Traffic**), you are downloading log messages in the Raw format.

### Viewing log messages in detail

From any log page, you can view detailed information about the log message in the log viewer table, located (by default) at the bottom of the page. Each page contains this log viewer table. The Log Viewer Table can contain the Archive tab, which allows you to see the archived version of the log message. The Archive tab only displays the archived log's details if archiving is enabled and logs are being archived by the FortiGate unit, but archived logs will also be recorded when using a FortiAnalyzer unit or the FortiCloud service.

When you are viewing traffic log messages, some of the categories (such as 'Application Name') have entries that can be selected to open a dialog box containing FortiGuard information about the entry. From within the dialog box, you can select the Reference link and go directly to the corresponding FortiGuard page, which contains additional information.

Viewing logs in Raw format allows you to view all log fields at once, as well as have a log file available regardless of whether you are archiving logs or not. You download the log file by selecting **Download Log**. The log file is named in the following format: <log_type><log_location><log_date/time>.<log_number>.log. For example, SystemEventLog-disk-2012-09-19T12_13_46.933949.log, which is an event log. The time period is the day and month of when the log was downloaded, not the time period of the log messages within the file itself.

### Quarantine

Within the Log & Report menu, you can view detailed information about each quarantined file. The information can either be sorted or filtered, depending on what you want to view.

You must enable quarantine settings within an antivirus profile and the destination must be configured in the CLI using the `config antivirus quarantine` command. The destination can be either a FortiAnalyzer unit or local disk.

Sort the files by file name, date, service, status, duplicate count (DC), or time to live (TTL). Filter the list to view only quarantined files with a specific status or from a specific service.

The file quarantine list displays the following information about each quarantined file.

**Quarantine page**

Lists all files that are considered quarantined by the unit. On this page you can filter information so that only specific files are displayed on the page.

| GUI Item | Description |
|---|---|
| **Source** | Either **FortiAnalyzer** or **Local Disk**, depending where you configure to quarantined files to be stored. |
| **Sort by** | Sort the list. Choose from: **Status**, **Service**, **File Name**, **Date**, **TTL**, or **Duplicate Count**. Select **Apply** to complete the sort. |

| GUI Item | Description |
|---|---|
| **Filter** | Filter the list. Choose either **Status** (infected, blocked, or heuristics) or **Service** (IMAP, POP3, SMTP, FTP, HTTP, MM1, MM3, MM4, MM7, IM, or NNTP). Select **Apply** to complete the filtering. Heuristics mode is configurable through the CLI only.<br><br>If your unit supports SSL content scanning and inspection Service can also be IMAPS, POP3S, SMTPS, or HTTPS. For more information, see the Security Features chapter of the FortiOS Handbook. |
| **Apply** | Select to apply the sorting and filtering selections to the list of quarantined files. |
| **Delete** | Select to delete the selected files. |
| **Page Controls** | Use the controls to page through the list. |
| **Remove All Entries** | Removes all quarantined files from the local hard disk.<br><br>This icon only appears when the files are quarantined to the hard disk. |
| **File Name** | The file name of the quarantined file. When a file is quarantined, all spaces are removed from the file name, and a 32-bit checksum is performed on the file. The checksum appears in the replacement message but not in the quarantined file. The file is stored on the FortiGate hard disk with the following naming convention:<br><br><32bit_CRC>.<processed_filename><br><br>For example, a file named Over Size.exe is stored as 3fc155d2.oversize.exe. |
| **Date** | The date and time the file was quarantined, in the format dd/mm/yyyy hh:mm. This value indicates the time that the first file was quarantined if duplicates are quarantined. |
| **Service** | The service from which the file was quarantined (HTTP, FTP, IMAP, POP3, SMTP, MM1, MM3, MM4, MM7, IM, NNTP, IMAPS, POP3S, SMTPS, or HTTPS). |
| **Status** | The reason the file was quarantined: **infected**, **heuristics**, or **blocked**. |
| **Status Description** | Specific information related to the status, for example, “File is infected with “W32/Klez.h”” or “File was stopped by file block pattern.” |
| **DC** | Duplicate count. A count of how many duplicates of the same file were quarantined. A rapidly increasing number can indicate a virus outbreak. |

| GUI Item | Description |
|---|---|
| **TTL** | Time to live in the format hh:mm. When the TTL elapses, the FortiGate unit labels the file as EXP under the TTL heading. In the case of duplicate files, each duplicate found refreshes the TTL.<br><br>The TTL information is not available if the files are quarantined on a FortiAnalyzer unit. |
| **Upload status** | **Y** indicates the file has been uploaded to Fortinet for analysis, **N** indicates the file has not been uploaded.<br><br>This option is available only if the FortiGate unit has a local hard disk. |
| **Download** | Select to download the corresponding file in its original format.<br><br>This option is available only if the FortiGate unit has a local hard disk. |
| **Submit** | Select to upload a suspicious file to Fortinet for analysis.<br><br>This option is available only if the FortiGate unit has a local hard disk. |

### Customizing the display of log messages on the web-based manager

Customizing log messages on the web-based manager allows you to remove or add columns from the page and filter the information that appears. For example, you can view only log messages that appeared on December 4, between the hours of 8:00 and 8:30 am.

1. Select the submenu in **Log & Report** in which you want to customize the display of log messages, such as **Log & Report > Forward Traffic**.
2. Right click on the title bar at the top of any column, and uncheck a column title such as **Date/Time** to remove it from the interface. Check other columns to add them to the interface. When you are finished, click outside the menu and the page will refresh with the new column settings in place.
3. Choose a column you'd like to filter, and select the funnel icon next to the title of the column. For example, select the funnel in the Src (Source) column. In the text field, enter the source IP address 1.1.1.1 and then select the check box beside **NOT**.
   This filters out the all log messages that have the 1.1.1.1 source IP address in the source IP log field, such as the ones generated when running log tests in the CLI.
4. Select **OK** to save the customize settings, and then view the log messages on the page.
   Log messages that originate from the 1.1.1.1 source address will no longer appear in the list.

## How to download log messages and view them from on a computer

After recording some activity, you can download log messages to view them from a computer. This is can be very useful when in a remote location, or if you want to view log messages at your convenience, or to view packet logs or traffic logs.

1. In Log & Report, select the submenu that you want to download log messages from.
   For example, **Log & Report > Forward Traffic**.

2. Select the **Download Log** option and save the log file to your computer.
   The log file will be downloaded like any other file. Log file names contain their log type and date in the name, so it is recommended to create a folder in which to archive your log messages, as they can be sorted easily.
3. Open a text editor such as Notepad, open the log file, and then scroll to view all the log messages.
   You can easily search or scroll through the logs to see the information that is available.

## Log files and types

As the log messages are being recorded, log messages are also being put into different log files. The log file contains the log messages that belong to that log type, for example, traffic log messages are put in the traffic log file.

When downloading the log file from within **Log & Report**, the file name indicates the log type and the device on which it is stored, as well as the date, time, and a unique id for that log.

This name is in the format <logtype> - <logdevice> - <date> T <time> . <id>.log.

For example, AntiVirusLog-disk-2012-09-13T11_07_57.922495.log.

Below, each of the different log files are explained. Traffic and Event logs come in multiple types, but all contain the base type such as 'Event' in the filename.

**Log Types based on network traffic**

| Log Type | Description |
|---|---|
| **Traffic** | The traffic logs records all traffic to and through the FortiGate interface. Different categories monitor different kinds of traffic, whether it be forward, local, or sniffer. |
| **Event** | The event logs record management and activity events within the device in particular areas: System, Router, VPN, User, Endpoint, HA, WAN Opt./Cache, and WiFi. For example, when an administrator logs in or logs out of the web-based manager, it is logged both in System and in User events. |
| **Antivirus** | The antivirus log records virus incidents in Web, FTP, and email traffic. |
| **Web Filter** | The web filter log records HTTP FortiGate log rating errors including web content blocking actions that the FortiGate unit performs. |
| **Application Control** | The application log records application usage, monitoring or blocking as configured in the security profiles. |
| **Intrusion** | The intrusion log records attacks that are detected and prevented by the FortiGate unit. |
| **Email Filter** | The email filter log records blocking of email address patterns and content in SMTP, IMAP, and POP3 traffic. |

| Log Type | Description |
|---|---|
| **Vulnerability Scan** | The Vulnerability Scan (Netscan) log records vulnerabilities found during the scanning of the network. |
| **Data Leak Prevention** | The Data Leak Prevention log records log data that is considered sensitive and that should not be made public. This log also records data that a company does not want entering their network. |
| **VoIP** | The VoIP log records VoIP traffic and messages. It only appears if VoIP is enabled on the Administrator Settings page. |

## Log database and datasets

The log database, also known as the SQL log database, is used to store logs on FortiGate units that have a built-in hard disk. The log database uses Structured Query Lanaguage (SQL), specifically it uses SQLite which is an embedded Relational Database Management System (RDBMS).

If you have disabled SQL logging and have factory defaults on the FortiGate unit, and then you upgrade the firmware, the upgrade will automatically disable SQL logging. When this occurs, you must re-enable SQL logging manually.

The FortiGate unit creates a database table for each log type, when log data is recorded. If the FortiGate unit is not recording log data, it does not create log tables for that device.

If you want to view the size of the database, as well as the log database table entries, use the `get report sql status` command. This command displays the amount of free space that is available as well as the first and last log database entry time and date.

The output of the `get report sql status` command contains information similar to the following:

```
Database size: 294912
Free size in database: 0
Database Page Size: 8192
Entry number:
Event: 49
Traffic: 370
Attack: 2
AntiVirus: 4
WebFilter: 254
AntiSpam: 2
Netscan: 18
Total: 699
First entry time: 2012-09-10 11:41:02
Last entry time: 2012-09-13 02:59:59
```

The log database is not only used to store logs, but also used to extract the information for reports. Reports are built from datasets, which are SQL statements that tell the FortiGate unit how to extract the information from the database. You can create your own datasets; however, SQL knowledge is required. Default datasets are available for reports.

## Notifications about network activity

Alert email messages provide notification about activities or events logged. These email messages also provide notification about log severities that are recorded, such as a critical or emergency.

You can send alert email messages to up to three email addresses. Alert messages are also logged and can be viewed from the Event Log menu, in the System Event log file.

You can use the alert email feature to monitor logs for log messages, and to send email notification about a specific activity or event logged. For example, if you require notification about administrators logging in and out, you can configure an alert email that is sent whenever an administrator logs in and out. You can also base alert email messages on the severity levels of the logs.

Before configuring alert email, you must configure at least one DNS server if you are configuring with an Fully Qualified Domain Server (FQDN). The FortiGate unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server. You can also specify an IP address.

The default minimum log severity level is Alert. If the FortiGate unit collects more than one log message before an interval is reached, the FortiGate unit combines the messages and sends out one alert email.

## How to configure email notifications

The following explains how to configure an alert email notification for IPsec tunnel errors, firewall authentication failure, configuration changes and FortiGuard license expiry.

1. In **System > Advanced**, under **Email Service**, configure the SMTP server.
   The SMTP server settings allow the FortiGate unit to know exactly where the email will be sent from, as well as who to send it to. The SMTP server must be a server that does not support SSL/TLS connections; if the SMTP server does, the alert email configuration will not work. The FortiGate unit does not currently support SSL/TLS connections for SMTP servers.
2. In **Log & Report > Alert E-mail**, enter the source email in the Email From field, and up to three target addresses in the Email To fields.
3. Below the email entry, you can configure the email responses. By default, the **Send alert email for the following** is enabled. Select the check boxes beside **IPsec tunnel errors**, **Configuration changes** and **Firewall authentication failure**.
   These alerts will be sent to the email address specified when the trigger occurs. For example, a user attempts to connect to the branch office of the company but cannot; the FortiGate unit detects an IPsec tunnel error, records the event, and then sends the notice to the email address specified in the SMTP server settings.
4. Select **FortiGuard license expiry time:** and then enter 10 so that the email notification will be sent ten days prior to the FortiGuard license expiration.
   You can choose up to 100 days prior to when the license will expire. The default time is 15 days. By using this alert email notification, you can easily know when to send an re-registration request long before the expiry.

# Log devices

The FortiGate unit supports a variety of log devices, including the FortiCloud service and FortiAnalyzer units. This provides greater flexibility not only when choosing a log device, but also when your logging requirements need updating.

When you have developed a plan that meets your logging needs and requirements, you need to select the log device that is appropriate for that plan. A log device must be able to store all the logs you need, and if you require archiving those logs, you must consider what log devices support this option.

During this process of deciding what log device meets your needs and requirements, you must also figure out how to provide a backup solution in the event the log device that the FortiGate unit is sending logs to has become unavailable. A backup solution should be an important part of your log setup because it helps you to maintain all logs and prevents lost logs, or logs that are not sent to the log device. For example, a daily backup of log files to the FortiAnalyzer unit occurs at 5 pm.

Log devices provide a central location for storing logs recorded by the FortiGate unit. The following are log devices that the FortiGate unit supports:

- FortiGate system memory
- Hard disk or AMC
- SQL database (for FortiGate units that have a hard disk)
- FortiAnalyzer unit
- FortiCloud service
- Syslog server

These log devices, except for the FortiGate system memory and local hard disk, can also be used as a backup solution. For example, you can configure logging to the FortiGate unit's local disk, but also configure logging to a FortiCloud server and archive logs to both the FortiCloud server and a FortiAnalyzer unit.

If you are formatting a disk that contains more than just logs, all information on the disk will be lost.

## FortiGate unit's system memory and hard disk

The FortiGate unit's system memory and hard disk can store all log types, including log archives and traffic logs. Traffic logs and log archives are larger files, and need a lot of room when being logged by the FortiGate unit.

When the system memory is full, the FortiGate unit overwrites the oldest messages, and all log messages stored in memory are cleared when the FortiGate unit restarts. By default, logging to memory is enabled. This means that most of the time you will only need to modify the default settings to your network logging requirements. Real-time logging occurs whenever memory logging is enabled, and is enabled by default. Real-time logging means that the activity is being recorded as it happens.

All FortiGate units 100D and larger are capable of disk logging, but it is disabled by default, as it is not recommended. For flash memory-based units, constant rewrites to flash drives can reduce the lifetime and efficiency of the memory. For hard-disk units, it can affect performance under heavy strain. Therefore, disk

logging must be manually enabled in the CLI under `config log disk setting` to appear in the interface at all.

Models without a hard disk are not recommended for disk logging. For all units, disk logging must be enabled in the CLI. For some low-end and older models, disk logging is unavailable. Check a product's Feature Matrix for more information. In either case, Fortinet recommends using either a FortiAnalyzer unit or the FortiCloud service.

Local disk or memory logging is not required for you to configure logging to a FortiAnalyzer unit.

If you are registered with the FortiCloud service, your unit will log both locally and to the service by default. In order to configure the rate and time of uploads to the service, you must register a contract account for the FortiCloud service, which will also grant you additional space.

## FortiAnalyzer unit

The FortiAnalyzer unit can log all FortiGate features, which includes log archives. You can also configure the FortiGate unit to upload logs to the FortiAnalyzer unit at a scheduled time.

Encryption of the logs is supported by default and logs are sent using SSL VPN. When the FortiAnalyzer and FortiGate units have SSL encryption, both must choose a setting for the enc-algorithm command (CLI) for encryption to take place. By default, this is enabled and the default setting is a SSL communication with high and medium encryption algorithms. The setting that you choose must be the same for both.

FortiGate units can support logging to multiple FortiAnalyzer units. This logging solution is a backup redundancy solution, since logs are sent to all three units and whenever one of the FortiAnalyzer units fails, the others still carry on storing logs.

If you are using evaluation software FortiGate and FortiAnalyzer-VM images, you will only be able to use low-level encryption.

The FortiGate unit can also connect to a FortiAnalyzer unit using Automatic Discovery. Automatic Discovery is a method of establishing a connection to a FortiAnalyzer unit by using the FortiGate unit to find a FortiAnalyzer unit on the network. The Fortinet Discovery Protocol (FDP) is used to located the FortiAnalyzer unit. Both the FortiGate and FortiAnalyzer units must be on the same subnet to use FDP, and they must also be able to connect using UDP.

When you enable automatic discovery in the CLI, the FortiGate unit uses HELLO packets to locate any FortiAnalyzer units that are available on the network within the same subnet. When the FortiGate unit discovers a FortiAnalyzer unit, the FortiGate unit automatically enables logging to the FortiAnalyzer unit and begins sending log data.

## Syslog server

A Syslog server is a remote computer running syslog software. Syslog is a standard for forwarding log messages in an IP network, and can be used when considering a log backup solution for your network logging requirements. Logs that are generated in real-time are sent to the syslog server in real time with no queueing, so it can be an ideal solution for comprehensive logging, or collecting logs for later systematic analysis.

FortiGate units support the reliable syslog feature, which is based on RFC 3195. Reliable syslog logging uses TCP, which ensures that connections are set up, including that packets are transmitted.

There are several profiles available for reliable syslog, but only the RAW profile is currently supported on the FortiGate units. The RAW profile is designed to provide a high-performance, low-impact footprint using essentially the same format as the existing UDP-based syslog service. The reliable syslog feature is available on FortiGate units running FortiOS 4.0 MR1 and higher.

When enabling the reliable syslog (available only in the CLI), TCP is used. The feature is disabled by default, and when enabled, the FortiGate unit automatically changes the port number to TCP 601. This is based on RFC 3195. The default port for syslog is port 514.

If you are using the local hard disk on a device for WAN Optimization, it will not prevent you from logging to remote FortiAnalyzer devices or Syslog servers. Some models have two hard disks, allowing both local logging and Wan Opt.

If you have Virtual Domains configured, each VDOM may only be assigned one FortiAnalyzer device and one Syslog server, by overriding the global configuration. The root VDOM is not limited in this way.

## How to choose a log device for your network topology

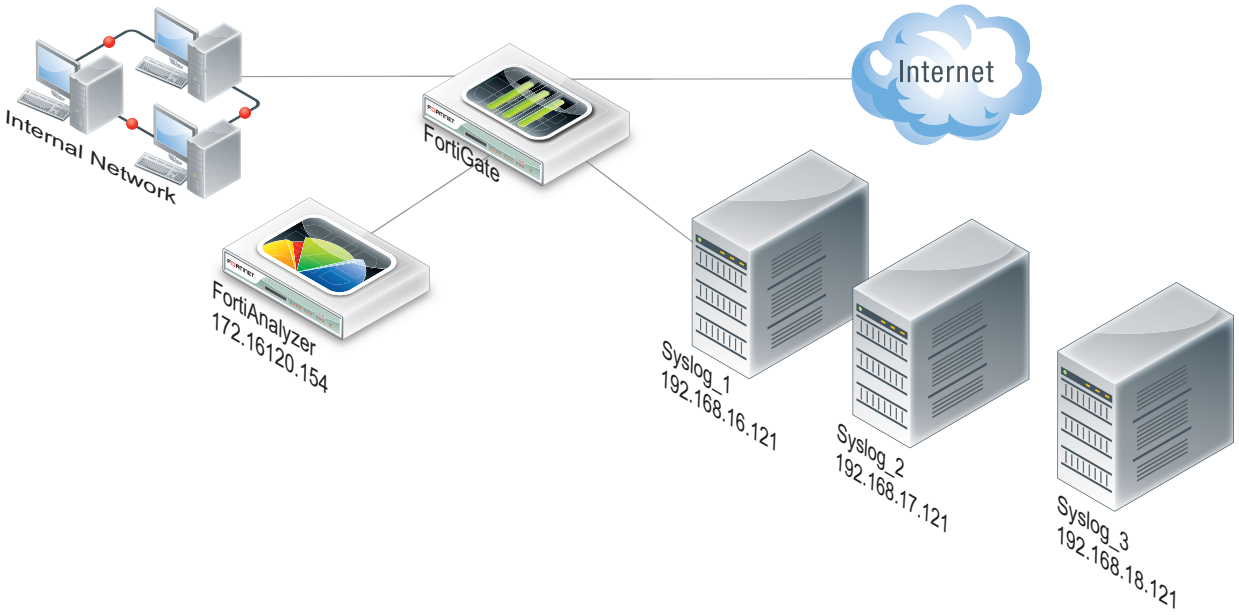
When planning the log requirements, you must also consider your network's topology and whether archiving is required, such as if there is a legal requirement to keep a historical record of network activity. The following explains what steps to take when choosing a log device for your specific network topology.

1. **What is the scope of your network topology?**
   If it is a SOHO/SMB network, then logging to the FortiGate unit's local hard disk or the default FortiCloud service would be efficient. If the network topology is a large enterprise, you will need FortiAnalyzer units, a FortiCloud contract, Syslog servers, or any combination.
2. **Is archiving required?**
   If the network activity that is being logged needs to be archived, then, depending on your network topology, you would choose a FortiAnalyzer unit. FortiAnalyzer units store archives in the same way that FortiGate units do, but are able to store large amounts of logs and archives.
3. **When troubleshooting, you may want to log a larger amount of traffic; how much storage space will you need?**
   Logs can be configured to roll, which is similar to zipping a file; this will lower the space requirements needed to contain them. You can also download logs from the FortiGate unit and save them on a server or on a computer to view and access later, to prevent them from piling up and being overwritten. If you're regularly logging large amounts of traffic, you should consider a FortiAnalyzer or FortiCloud account .
4. **Should I invest in a log device that can grow as my network grows?**
   All networks grow, so investing in a device that can grow with your network and that can be expanded is a good investment. For example, if you currently have a SOHO/SMB topology, but see growth already starting, a FortiAnalyzer unit would be best. A FortiAnalyzer unit provides ample storage space, and you can add two more FortiAnalyzer units to access additional storage and create a redundancy log backup solution.

## How to create a backup solution for logging

The following helps to explain how to create a log backup solution for a small network topology. This example has one FortiAnalyzer unit and a subscription to the FortiCloud Service.

**Example of an integrated FortiAnalyzer unit and Syslog servers in a network**




1. Log in to the CLI and modify what features will be logged to the FortiAnalyzer unit as well as the settings to the default log device, the FortiGate unit's hard drive.
   By default, the FortiGate unit logs to either the system memory or hard drive, whichever is available on the FortiGate unit. Low-end FortiGate units may have logging disabled by default.
2. In the CLI, use the `config log fortianalyzer setting` command to configure logging to the FortiAnalyzer unit.
   You can only configure log settings for the FortiAnalyzer unit in the CLI. Configuring to upload logs to a FortiAnalyzer unit can be configured in both the CLI and web-based manager.
3. In the CLI, configure the settings for the Syslog server; also enable reliable syslog as well.
   Reliable syslog verifies that logs are sent to the syslog server. When you enable this setting, the default port becomes port 601.

# Reports

Reports provide a clear, concise overview of what is happening on your network based on log data, and can be customized to serve different purposes. There are three types of reports supported by the FortiGate: FortiOS Reports, FortiCloud Reports, and FortiAnalyzer Reports.

FortiOS Reports are generated and configured on the FortiGate unit itself, FortiCloud Reports are created and configured on the FortiCloud site and mirrored to the connected FortiGate for viewing, and FortiAnalyzer reports

are created and configured on a FortiAnalyzer unit. For more information about those reports, see the FortiAnalyzer Administration Guide.

In order to create FortiOS Reports on a device, disk logging must be enabled. Not all devices are capable of disk logging; check the Feature Matrix to see if your unit has a hard disk. Once disk logging has been enabled, Local Reports can then be enabled in **System > Feature Visibility** in order to view and edit reports.

### What are FortiOS reports?

FortiOS reports are created from logs stored on the FortiGate unit's hard drive. These reports, generated by the FortiGate unit itself, provide a central overview of traffic and security features on the FortiGate. A default FortiOS report, called the FortiGate Security Feature Daily Activity Report, is available for you to use or modify to your requirements. The default report compiles security feature activity from various security-related logs, such as virus and attack logs. You can quickly and easily create your own report from within the management interface.

### What you can do with the default FortiOS report

On the **Log & Report > Local Reports** page, you can set the frequency and timing of auto-generated reports.

You can select **Run Now**on the **Local Reports** page to immediately create a report with the current layout and design. More complex reports may take longer to generate. After generating a report, you can view it by selecting it from the list below **Run Now**.

Historical reports will be marked as 'Scheduled' if created automatically, or 'On Demand' if created by selecting **Run Now**.

### What are FortiCloud reports?

FortiCloud reports are created from logs stored on the FortiCloud log management service. An active FortiCloud Service Subscription is required in order to view, configure, or use these reports. They are generated by FortiCloud according to a schedule you set, and then mirrored to the FortiGate interface and can be viewed at **Log & Report > FortiCloud Reports**, which may not appear in the interface until a report is created. If you wish to configure the report design or structure, you will have to do so from the FortiCloud portal website.

See the FortiCloud Administration Guide for more information about using and configuring FortiCloud reports.

## Best Practices: Log management

When the FortiGate unit records FortiGate activity, valuable information is collected that provides insight into how to better protect network traffic against attacks, including misuse and abuse. There is a lot to consider before enabling logging on a FortiGate unit, such as what FortiGate activities to enable and which log device is best suited for your network's logging needs. A plan can help you in deciding the FortiGate activities to log, a log device, as well as a backup solution in the event the log device fails.

This plan should provide you with an outline, similar to the following:

- what FortiGate activities you want and/or need logged (for example, security features)
- the logging device best suited for your network structure
- if you want or require archiving of log files
- ensuring logs are not lost in the event a failure occurs.

After the plan is implemented, you need to manage the logs and be prepared to expand on your log setup when the current logging requirements are outgrown. Good log management practices help you with these tasks.

Log management practices help you to improve and manage logging requirements. Logging is an ever-expanding tool that can seem to be a daunting task to manage. The following management practices will help you when issues arise, or your logging setup needs to be expanded.

1. Revisit your plan on a yearly basis to verify that your logging needs are being met by your current log setup. For example, your company or organization may require archival logging, but not at the beginning of your network's lifespan. Archival logs are stored on a FortiGate unit's local hard drive, a FortiAnalyzer unit, or a FortiCloud server, in increasing order of size.
2. Configure an alert message that will notify you of activities that are important to be aware about. For example: if a branch office does not have a FortiGate administrator, you will need to know at all times that the IPsec VPN tunnel is still up and running. An alert email notification message can be configured to send only if IPsec tunnel errors occur.
3. If your organization or company uses peer-to-peer programs such as Skype or other instant messaging software, use the Applications FortiView dashboard, or the Executive Summary's report widget (Top 10 Application Bandwidth Usage Per Hour Summary) to help you monitor the usage of these types of instant messaging software. These widgets can help you in determining how these applications are being used, including if there is any misuse and abuse. Their information is taken from application log messages; however, application log messages should be viewed as well since they contain the most detailed information.
4. Ensure that your backup solution is up-to-date. If you have recently expanded your log setup, you should also review your backup solution. The backup solution provides a way to ensure that all logs are not lost in the event that the log device fails or issues arise with the log device itself.

# Logging and reporting for small networks

This section explains how to configure the FortiGate unit for logging and reporting in a small office or SOHO/SMB network. To properly configure this type of network, you will be modifying the default log settings, as well as the default FortiOS report.

The following procedures are examples and can be used to help you when configuring your own network's log topology. Since some of these settings must be modified or enabled or disabled in the CLI, it is recommended to review the FortiGate CLI Reference for any additional information about the commands used herein, as well as any that you would need to use in your own network's log topology.

## Modifying default log device settings

The default log device settings must be modified so that system performance is not compromised. The FortiGate unit, by default, has all logging of FortiGate features enabled, except for traffic logging. The default logging location will be either the FortiGate unit's system memory or hard disk, depending on the model. Units with a flash disk are not recommended for disk logging.

### Modifying the FortiGate unit's system memory default settings

When the FortiGate unit's default log device is its system memory, the following is modified for a small network topology. The following is an example of how to modify these default settings.

**To modify the default system memory settings**

1. Log in to the CLI.
2. Enter the following command syntax to modify the logging settings:

```
config log memory setting
   set status enable
end
```

3. The following example command syntax modifies which FortiGate features that are enabled for logging:

```
config log memory filter
   set forward-traffic enable
   set local-traffic enable
   set sniffer-traffic enable
   set anomaly enable
   set voip disable
   set multicast-traffic enable
   set dns enable
end
```

### Modifying the FortiGate unit's hard disk default settings

When the FortiGate unit's default log device is its hard disk, you need to modify those settings to your network's logging needs so that you can effectively log what you want logged. The following is an example of how to modify these default settings.

**To modify the default hard disk settings**

1. Log in to the CLI.
2. Enter the following command syntax to modify the logging settings:

```
config log disk setting
   set ips-archive disable
   set status enable
   set max-log-file-size 1000
   set storage FLASH
   set log-quota 100
   set report-quota 100
end
```

3. In the CLI, enter the following to disable certain event log messages that you do not want logged:

```
config log eventfilter
   set event enable
   set system enable
   set vpn disable
   set user enable
   set router disable
   set wan-opt disable
end
```

## Testing sending logs to the log device

After modifying both the settings and the FortiGate features for logging, you can test that the modified settings are working properly. This test is done in the CLI.

**To test sending logs to the log device**

1. In the CLI, enter the following command syntax:

```
diag log test
```

When you enter the command, the following appears:

```
generating a system event message with level - warning
generating an infected virus message with level - warning
generating a blocked virus message with level - warning
generating a URL block message with level - warning
generating a DLP message with level - warning
generating an IPS log message
generating an anomaly log message
generating an application control IM message with level - information
generating an IPv6 application control IM message with level - information
generating deep application control logs with level - information
generating an antispam message with level - notification
generating an allowed traffic message with level - notice
generating a multicast traffic message with level - notice
generating a ipv6 traffic message with level - notice
generating a wanopt traffic log message with level - notification
generating a HA event message with level - warning
generating netscan log messages with level - notice
generating a VOIP event message with level - information
generating a DNS event message with level - information
generating authentication event messages
```

```
generating a Forticlient message with level - information
generating a URL block message with level - warning
```

2. In the web-based interface, go to **Log & Report > System Events**, and view the logs to see some of the recently generated test log messages.
   You will be able to tell the test log messages from real log messages because they do not have “real” information; for example, the test log messages for the vulnerability scan contain the destination IP address of 1.1.1.1 or 2.2.2.2.

# Configuring the backup solution

A backup solution provides a way to ensure logs are not lost. The following backup solution explains logging to a FortiCloud server and uploading logs to a FortiAnalyzer unit. With this backup solution, there can be three simultaneous storage locations for logs, the first being the FortiGate unit itself, the FortiAnalyzer unit and then the FortiCloud server.

## Configuring logging to a FortiCloud server

The FortiCloud server can be used as a redundant backup, or your primary logging solution. The following assumes that this service has already been registered, and a subscription has been purchased for expanded space. The following is an example of how to these settings are configured for a network’s log configuration. You need to have access to both the CLI and the web-based manager when configuring uploading of logs. The upload time and interval settings can be configured in the web-based interface.

**To configure logging to the FortiCloud server**

1. Go to **Dashboard** and click **Login** next to **FortiCloud** in the **License Information** widget.
2. Enter your username and password, and click **OK**. (Or register, if you have not yet done so.)
3. Logs will automatically be uploaded to FortiCloud as long as your FortiGate is linked to your FortiCloud account.
4. To configure the upload time and interval, go to **Log & Report > Log Settings**.
5. Under the Logging and Archiving header, you can select your desired upload time.

With FortiCloud you can easily store and access FortiGate logs that can give you valuable insight into the health and security of your network.

## Configuring uploading logs to the FortiAnalyzer unit

The logs will be uploaded to the FortiAnalyzer unit at a scheduled time. The following is an example of how to upload logs to a FortiAnalyzer unit.

**To upload logs to a FortiAnalyzer unit**

1. Go to **Log & Report > Log Settings**.
2. In the **Remote Logging and Archiving** section, select the check box beside **Send Logs to FortiAnalyzer/FortiManager.**
3. Select **FortiAnalyzer (Daily at 00:00)**.
4. Enter the FortiAnalyzer unit’s IP address in the **IP Address** field.

5. To configure the daily upload time, open the CLI.
6. Enter the following to configure when the upload occurs, and the time when the unit uploads the logs:

```
config log fortianalyzer setting
   set upload-interval {daily | weekly | monthly}
   set upload-time <hh:mm>
end
```

7. To change the upload time, in the web-based manager, select **Change** beside the upload time period, and then make the changes in the Upload Schedule window. Select **OK**.

## Testing uploading logs to a FortiAnalyzer unit

You should test that the FortiGate unit can upload logs to the FortiAnalyzer unit, so that the settings are configured properly.

**To test the FortiAnalyzer upload settings**

1. Go to **Log & Report > Log Settings.**
2. In the **Logging and Archiving** section, under **Send Logs to FortiAnalyzer/FortiManager**, change the time to the current time by selecting **Change**.
   For example, the current time is 11:10 am, so **Change** now has the time 11:10.
3. Select **OK**.

The logs will be immediately sent to the FortiAnalyzer unit, and will be available to view from within the FortiAnalyzer's interface.

# Logging and reporting for large networks

This section explains how to configure the FortiGate unit for logging and reporting in a larger network, such as an enterprise network. To set up this type of network, you are modifying the default log settings, and you are also modifying the default report.

The following procedures are examples and can be used to help you when configuring your own network's log topology.

Since some of these settings must be modified or enabled or disabled in the CLI, it is recommended to review the FortiGate CLI Reference for any additional information about the commands used herein, as well as any that you would need to use in your own newtork's log topology.

## Modifying default log device settings

The default log device settings must be modified so that system performance is not compromised. The FortiGate unit, by default, has all logging of FortiGate features enabled and well as logging to either the FortiGate unit's system memory or hard disk, depending on the model.

### Modifying multiple FortiGate units' system memory default settings

When the FortiGate unit's default log device is its system memory, you can modify it to fit your log network topology. In this topic, the following is an example of how you can modify these default settings.

**To modify the default system memory settings**

1. Log in to the CLI.
2. Enter the following command syntax to modify the logging settings:

```
config log memory setting
   set status enable
end
```

3. Enter the following command syntax to modify the FortiGate features that are enabled for logging:

```
config log memory filter
   set forward-traffic enable
   set local-traffic enable
   set sniffer-traffic enable
   set anomaly enable
   set voip enable
   set multicast-traffic enable
   set dns enable
end
```

4. Repeat steps 2 and 3 for the other FortiGate units.
5. Test the modified settings using the procedure below.

## Modifying multiple FortiGate units' hard disk default log settings

You will have to modify each FortiGate unit's hard disk default log settings. The following is an example of how to modify these default settings.

**To modify the default hard disk settings**

1. Log in to the CLI.
2. Enter the following command syntax to modify the logging settings:

```
config log disk setting
   set ips-archive disable
   set status enable
   set max-log-file-size 1000
   set storage Internal
   set log-quota 100
   set report-quota 100
end
```

3. In the CLI, enter the following to disable certain event log messages that you do not want logged:

```
config log eventfilter
   set event enable
   set system enable
   set vpn enable
   set user enable
   set router disable
   set wan-opt disable
end
```

4. Repeat the steps 2 to 4 for the other FortiGate units.
5. Test the modified settings using the procedure below.

## Testing the modified log settings

After modifying both the settings and the FortiGate features for logging, you can test that the modified settings are working properly. This test is done in the CLI.

**To test sending logs to the log device**

1. In the CLI, enter the following command syntax:

```
diag log test
```

When you enter the command, the following appears:

```
generating a system event message with level - warning
generating an infected virus message with level - warning
generating a blocked virus message with level - warning
generating a URL block message with level - warning
generating a DLP message with level - warning
generating an IPS log message
generating an anomaly log message
generating an application control IM message with level - information
generating an IPv6 application control IM message with level - information
generating deep application control logs with level - information
generating an antispam message with level - notification
```

```
generating an allowed traffic message with level - notice
generating a multicast traffic message with level - notice
generating a ipv6 traffic message with level - notice
generating a wanopt traffic log message with level - notification
generating a HA event message with level - warning
generating netscan log messages with level - notice
generating a VOIP event message with level - information
generating a DNS event message with level - information
generating authentication event messages
generating a Forticlient message with level - information
generating a URL block message with level - warning
```

2. In the web-based interface, go to **Log & Report > System Events**, and view the logs to see some of the recently generated test log messages.
   You will be able to tell the test log messages from real log messages because they do not have “real” information; for example, the test log messages for the vulnerability scan contain the destination IP address of 1.1.1.1 or 2.2.2.2.

# Configuring the backup solution

Even though you are logging to multiple FortiAnalyzer units, this is more of a redundancy solution rather than a complete backup solution in this example.

The multiple FortiAnalyzer units act similar to a HA cluster, since if one FortiAnalyzer unit fails, the others continue storing the logs they receive. In a backup solution, the logs are backed up to another secure location if something happens to the log device.

A good alternate or redundant option is the FortiCloud service, which can provide secure online logging and management for multiple devices.

## Configuring logging to multiple FortiAnalyzer units

The following example shows how to configure logging to multiple FortiAnalyzer units. Configuring multiple FortiAnalyzer units is quick and easy; however, you can only configure up to three FortiAnalyzer units per FortiGate unit.

**To configure multiple FortiAnalyzer units**

1. In the CLI, enter the following command syntax to configure the first FortiAnalyzer unit:

```
config log fortianalyzer setting
   set status enable
   set server 172.20.120.22
   set max-buffer-size 1000
   set buffer-max-send 2000
   set address-mode static
   set conn-timeout 100
   set monitor-keepalive-period 120
   set monitor-failure-retry-period 2000
end
```

2. Disable the features that you do not want logged, using the following example command syntax. You can view the CLI Reference to see what commands are available.

```
config log fortianalyzer filter
   set forward-traffic (enable | disable)
   ...
end
```

3. Enter the following commands for the second FortiAnalyzer unit:

```
   config log fortianalyzer2 setting
      set status enable
      set server 172.20.120.23
      set max-buffer-size 1000
      set buffer-max-send 2000
      set address-mode static
      set conn-timeout 100
      set monitor-keepalive-period 120
      set monitor-failure-retry-period 2000
end
```

4. Disable the features that you do not want logged, using the following example command syntax.

```
config log fortianalyzer2 filter
   set event (enable | disable)
   ...
end
```

5. Enter the following commands for the last FortiAnalyzer unit:

```
   config log fortianalyzer3 setting
      set status enable
      set server 172.20.120.23
      set max-buffer-size 1000
      set buffer-max-send 2000
      set address-mode static
      set conn-timeout 100
      set monitor-keepalive-period 120
      set monitor-failure-retry-period 2000
end
```

6. Disable the features that you do not want logged, using the following example command syntax.

```
config log fortianalyzer3 filter
   set voip (enable | disable)
   ...
end
```

7. Test the configuration by using the procedure, "Testing the modified log settings".
8. On the other FortiGate units, configure steps 1 through 6, ensuring that logs are being sent to the FortiAnalyzer units.

## Configuring logging to the FortiCloud server

The FortiCloud server can be used as a redundant backup, or your primary logging solution. The following assumes that this service has already been registered, and a subscription has been purchased for expanded space. The following is an example of how to these settings are configured for a network's log configuration. You need to have access to both the CLI and the web-based manager when configuring uploading of logs. The upload time and interval settings can be configured in the web-based interface.

**To configure logging to the FortiCloud server**

1. Go to **Dashboard** and click **Login** next to **FortiCloud** in the License Information widget.
2. Enter your username and password, and click **OK**. (Or register, if you have not yet done so.)
3. Logs will automatically be uploaded to FortiCloud as long as your FortiGate is linked to your FortiCloud account.
4. To configure the upload time and interval, go to **Log & Report > Log Settings**.
5. Under the **Remote Logging and Archiving** header, you can select your desired upload time.
6. With FortiCloud you can easily store and access FortiGate logs that can give you valuable insight into the health and security of your network.

# Advanced logging

This section explains how to configure other log features within your existing log configuration. You may want to include other log features after initially configuring the log topology because the network has either outgrown the initial configuration, or you want to add additional features that will help your network's logging requirements.

The following topics are included in this section:



## Log backup and restore tools

Local disk logs can now be backed up and restored to local files, using CLI commands:

```
execute log backup <filename>
execute log restore <filename>
```

Restoring logs will wipe the current log and report content off the disk.

Logs can also now be exported to a USB storage device, as LZ4 compressed files, from both CLI and GUI. When you insert a USB drive into the FortiGate's USB port, the USB menu will appear in the GUI. The menu shows the amount of storage on the USB disk, and the log file size, and you can select **Copy to USB** to copy the log data to the drive.

## Configuring logging to multiple Syslog servers

A single remote Syslog server can be configured in the GUI, in **Log & Report > Log Settings**, but for a larger network, you will have to configure it in the CLI.

When configuring multiple Syslog servers (or one Syslog server), you can configure reliable delivery of log messages from the Syslog server. Configuring of reliable delivery is available only in the CLI.

If VDOMs are enabled, you can configure separate FortiAnalyzer unit or Syslog server for each VDOM.

**To enable logging to multiple Syslog servers:**

1. Log in to the CLI.
2. Enter the following commands:

```
config log syslogd setting
   set csv {disable | enable}
   set facility <facility_name>
   set port <port_integer>
   set reliable {disable | enable}
   set server <ip_address>
   set status {disable | enable}
end
```

3. Enter the following commands to configure the second Syslog server:

```
config log syslogd2 setting
   set csv {disable | enable}
   set facility <facility_name>
   set port <port_integer>
   set reliable {disable | enable}
   set server <ip_address>
   set status {disable | enable}
end
```

4. Enter the following commands to configure the third Syslog server:

```
config log syslogd3 setting
   set csv {disable | enable}
   set facility <facility_name>
   set port <port_integer>
   set reliable {disable | enable}
   set server <ip_address>
   set status {disable | enable}
end
```

5. Enter the following commands to configure the fourth Syslog server:

```
config log syslogd4 setting
   set csv {disable | enable}
   set facility <facility_name>
   set port <port_integer>
   set reliable {disable | enable}
   set server <ip_address>
   set status {disable | enable}
end
```

Most FortiGate features are, by default, enabled for logging. You can disable individual FortiGate features you do not want the Syslog server to record, as in this example:

```
config log syslogd filter
   set local-traffic {enable | disable}
   set severity {alert | critical | debug | emergency | error | information |
       notification | warning}
end
```

## Using Automatic Discovery to connect to a FortiAnalyzer unit

Automatic Discovery can be used if the FortiAnalyzer unit is on the same network.

**To connect using automatic discovery**

1. Log in to the CLI.
2. Enter the following command syntax:

```
config log fortianalyzer setting
   set status enable
   set server <ip_address>
   set gui-display enable
   set address-mode auto-discovery
end
```

If your FortiGate unit is in Transparent mode, the interface using the automatic discovery feature will not carry traffic. For more information about how to enable the interface to also carry traffic when using the automatic discovery feature, see the Fortinet Knowledge Base article, Fortinet Discovery Protocol in Transparent mode.

The FortiGate unit searches within the same subnet for a response from any available FortiAnalyzer units.

## Activating a FortiCloud account for logging purposes

When you subscribe to FortiCloud, you can configure to send logs to the FortiCloud server. The account activation can be done within the web-based manager, from the **License Information** widget located in **Dashboard**.

From this widget, you can easily create a new account, or log in to the existing account. From within the License Information widget, after the account is activated, you can go directly to the FortiCloud web portal, or log out of the service if you are already logged in.

**To activate a FortiCloud account for logging purposes:**

The following assumes that you are already at **Dashboard** and that you have located the License Information widget.

1. In the License Information widget, select **Activate** in the **FortiCloud** section.
   The Registration window appears. From this window, you create the login credentials that you will use to access the account.
2. Select **Create Account** and enter then information for the login credentials.
   After entering the login credentials, you are automatically logged in to your FortiCloud account.
3. Check that the account has been activated by viewing the account status from the License Information widget.

If you need more space, you can subscribe to the 200Gb FortiCloud service by selecting **Upgrade** in the **FortiCloud** section of the widget.

## Viewing log storage space

The **Log & Report > Log Settings** GUI page displays two charts to visualize disk space: Disk Usage, which is a pie-chart illustrating the Free/Used space on the internal hard drive, and Historical Disk Usage, which displays the volume of disk logging activity over time. These charts may not be visible if disk logging is disabled.

The `diag sys logdisk usage` command allows you to view detailed information about how much space is currently being used for logs. This is useful when you see a high percentage, such as 92 percent for the disk's capacity. The FortiGate unit uses only 75 percent of the available disk capacity to avoid a high storage amount so when there is a high percentage, it refers to the percentage of the 75 percent that is available. For example, 92 percent of the 75 percent is available.

The following is an example of what you may see when you use `diag sys logdisk usage` command on a unit with no VDOMs configured:

```
diag sys logdisk usage
```

The following appears:

```
Total HD usage: 176MB/3011 MB
Total HD logging space: 22583MB
Total HD logging space for each vdom: 22583MB
HD logging space usage for vdom "root": 30MB/22583MB
```

## Customizing and filtering log messages

When viewing log messages, you may want to customize and filter the information that you are seeing in the Log & Report menu (for example, **Log & Report > Forward Traffic**). Filtering and customizing the display provides a way to view specific log information without scrolling through pages of log messages to find the information.

Customizing log messages is the process of removing or adding columns to the log display page, allowing you to view certain desired information. The most columns represent the fields from within a log message, for example, the user column represents the user field, as well as additional information. If you want to reset the customized columns on the page back to their defaults, you need to select **Reset All Columns** within the column title right-click menu.

Filtering information is similar to customizing, however, filtering allows you to enter specific information that indicates what should appear on the page. For example, including only log messages that appeared on February 24, between the hours of 8:00 and 8:30 am.

### To customize and filter log messages

The following is an example that displays all traffic log messages that originate from the source IP address 172.20.120.24, as well as displaying only the columns:

- OS Name
- OS Version
- Policy ID
- Src (Source IP)

The following assumes that you are already on the page of the log messages you want to customize and filter. In this example, the log messages that we are customizing and filtering are in **Log & Report > Forward Traffic**.

1. On the **Forward Traffic** page, right click anywhere on a column title.
2. Right click on a column title, and mouse over **Column Settings** to open the list.
3. Select each checkmarked title to uncheck it and remove them all from the displayed columns.
4. Scroll down to the list of unchecked fields and select 'OS Name', 'OS Version', 'Policy ID', and 'Src' to add checkmarks next to them.
5. Click outside the menu, and wait for the page to refresh with the new settings in place.
6. Select the funnel icon next to the word Src in the title bar of the Src column.
7. Enter the IP you want displayed (in this example, 172.20.120.24) in the text box.
8. Click **Apply**, and wait for the page to reload.

## Viewing logs from the CLI

You can easily view log messages from within the CLI. In this example, we are viewing DLP log messages.

1. Log in to the CLI and then enter the following to configure the display of the DLP log messages.

   ```
   execute log filter category 9
   execute log filter start-line 1
   execute log filter view-lines 20
   ```

   The customized display of log messages in the CLI is similar to how you customize the display of log messages in the web-based manager. For example, `category 9` is the DLP log messages, and the `start-line` is the first line in the log database table for DLP log messages, and there will be 20 lines (`view-lines 20`) that will display.

2. Enter the following to view the log messages:

   ```
   execute log display
   ```

   The following appears below execute log display:

   ```
   600 logs found
   20 logs returned
   ```

   along with the 20 DLP log messages.

## Configuring NAC quarantine logging

NAC quarantine log messages provide information about what was banned and quarantined by a Antivirus profile. The following explains how to configure NAC quarantine logging and enable it on a policy. This procedure assumes the Antivirus profile is already in place.

**To configure NAC quarantine logging**

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select the policy that you want to apply the Antivirus profile to, and then select **Edit**.
3. Within the Security Profiles section, enable **Antivirus** and then select the profile from the drop-down list.
4. Select **OK**.

5. Log in to the CLI.
6. Enter the following to enable NAC quarantine in the DLP sensor:

```
config antivirus profile
   edit <profile_name>
      config nac-quar log enable
   end
```

## Logging local-in policies

Local-in security policies are policies the control the flow of internal traffic, and can be used to broaden or restrict an administrator's access privileges. These local-in policies can also be configured to log traffic and activity that the policies control.

You can enable logging of local-in policies in the CLI, with the following commands:

```
config system global
   set gui-local-in-policy enable
end
```

The Local-In Policy page will then be available in **Policy & Objects > Local In Policy**. You can configure what local-in traffic to log in the CLI, or in **Log & Report > Log Settings**, under **Local Traffic Logging**.

When deciding what local-in policy traffic you want logged, consider the following:

**Special Traffic**

| Traffic activity | Traffic Direction | Description |
|---|---|---|
| **FortiGuard update annoucements** | IN | All push announcements of updates that are coming from the FortiGuard system. For example, IPS or AV updates. |
| **FortiGuard update requests** | OUT | All updates that are checking for antivirus or IPS as well as other FortiGuard service updates. |
| **Firewall authentication** | IN | The authentication made using either the web-based manager or CLI. |
| **Central management (a FortiGate unit being managed by a FortiManager unit)** | IN | The access that a FortiManager has managing the FortiGate unit. |
| **DNS** | IN | All DNS traffic. |
| **DHCP/DHCP Relay** | IN | All DHCP and/or DHCP Relay traffic. |

| Traffic activity | Traffic Direction | Description |
|---|---|---|
| **HA (heart beat sync policy)** | IN/OUT | For high-end platforms with a backplane heart beat port. |
| **HA (Session sync policy)** | IN/OUT | This will get information from the CMDB and updated by session sync daemon. |
| **CAPWAP** | IN | This activity is logged only when a HAVE_CAPWAP is defined. |
| **Radius** | IN | This is recorded only within FortiCarrier. |
| **NETBIOS forward** | IN | Any interface that NETBIOS forward is enabled on. |
| **RIP** | IN | |
| **OSPF** | IN | |
| **VRRP** | IN | |
| **BFD** | IN | |
| **IGMP** | IN | This is recorded only when PIM is enabled. |
| **PIM** | IN | This is recorded only when PIM is enabled. |
| **BGP** | IN | This is recorded only when config bgp and bgp neightbor is enabled in the CLI. |
| **WCCP policy** | IN | Any interface that WCCP is enabled; however, if in Cache mode, this is not recorded because it is not available. |
| **WAN Opt/ Web Cache** | IN | Any interface where WAN Opt is enabled. |
| **WANOpt Tunnel** | IN | This is recorded when HAVE_WANOPT is defined. |
| **SSL-VPN** | IN | Any interface from a zone where the action in the policy is SSL VPN. |
| **IPSEC** | IN | |
| **L2TP** | IN | |
| **PPTP** | IN | |
| **VPD** | IN | This is recorded only when FortiClient is enabled. |
| **Web cache db test facility** | IN | This is recorded only when WA_CS_REMOTE_TEST is defined. |
| **GDBserver** | IN | This is recorded only when debug is enabled. |

# Tracking specific search phrases in reports

It is possible to use the Web Filter to track specific search keywords and phrases and record the results for display in the report.

You should verify that the web filter profile you are using indicates what search phrases you want to track and monitor, so that the report includes this information.

1. **Log in to the CLI and enter show webfilter profile default.**
   This provides details about the webfilter profile being used by the security policy. In this example, the details (shown in the following in bold) indicate that safe search is enabled, but not specified or being logged.

```
show webfilter profile default
   config webfilter profile
      edit "default"
         set comment "default web filtering"
         set inspection-mode flow-based
         set options https-scan
         set post-action comfort
            config web
               set safe-search url
            end
            config ftgd-wf
               config filters
                  edit 1
                     set action block
                     set category 2
                  next
                  edit 2
                     set action block
                     set category 7
                  next
                  edit 3
                     set action block
                     set category 8
```

2. **Enter the following command syntax so that logging and the keyword for the safe search will be included in logging.**

```
config webfilter profile
   edit default
      config web
         set log-search enable
         set keyword-match "fortinet" "easter" "easter bunny"
      end
   end
```

3. **To test that the keyword search is working, go to a web browser and begin searching for the words that were included in the webfilter profile, such as easter.**
   You can tell that the test works by going to **Log & Report > Forward Traffic** and viewing the log messages.

# Interpreting and configuring FSSO syslog log messages

There are two syslog message formats: default and verbose. Verbose must be manually enabled as described below, but provides more general information.

## Default syslog message format

The default FSSO syslog message format has no header, and is based on the specifications of RFC 3164. Messages only have two values, `PRI` (Priority) and `MSG` (Message), in the format of `<PRI>MSG`.

The content of `PRI` is as described in RFC 3164, but with specific parameters: the Facility value is always 1 (USER), unless 'Log logons in separate log' is enabled in the FSSO Collector Agent settings. In that case, those logon messages will have a Facility value of 4 or 10 (AUTH). The Severity value always matches the internal severity value of the log. `PRI` is enclosed in < > with no space following before `MSG`.

## Verbose syslog message format

Verbose is a secondary message format that provides more information, including timestamp (with timezone).

In verbose mode, the log message follows the specifications of RFC 5424:

```
<PRI>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA/SD-ID
MSG
```

`PRI` is formatted as described above in the default format.

Verbose FSSO syslog messages do not contain any data for `MSGID`, or `STRUCTURED-DATA`, so both of those two messages are recorded as a single hyphen character "`-`".

`APP-NAME` always appears as "`collectoragent`".

The other values are formatted as described in RFC 5424.

## Enabling verbose syslog message mode

In order to enable the verbose syslog message mode, you must modify the registry on the PC that is hosting the FSSO Collector Agent.

In 64-bit Windows, locate the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fortinet\FSAE\collectoragent
```

In 32-bit Windows, locate the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\collectoragent
```

Under this registry path, create a new DWORD (32bit) Value named `syslog_using_rfc`, and set its value to 1.

# Troubleshooting and logging

This section explains how to troubleshoot logging configuration issues, as well as connection issues, that you may have with your FortiGate unit and a log device. This section also contains information about how to use log messages when troubleshooting issues that are about other FortiGate features, such as VPN tunnel errors.

## Using log messages to help in troubleshooting issues

Log messages can help when troubleshooting issues that occur, since they can provide details about what is occurring. The uses and methods for involving logging in troubleshooting vary depending on the problem. The following are examples of how log messages can assist when troubleshooting networking issues.

### Using IPS packet logging in diagnostics

This type of logging should only be enabled when you need to know about specific diagnostic information, for example, when you suspect a signature is triggered by a false positive. These log messages can help troubleshoot individual problems with misidentified or missing packets and network intrusions involving malicious packets.

**To configure IPS packet logging**

1. Go to **Security Profiles > Intrusion Protection**.
2. Select the IPS sensor that you want to enable IPS packet logging on, and then select **Edit**.
3. In the filter options, enable **Packet Logging**.
4. Select **OK**.

If you want to configure the packet quota, number of packets that are recorded before alerts and after attacks, use the following procedure.

**To configure additional settings for IPS packet logging**

1. Log in to the CLI.
2. Enter the following to start configuring additional settings:

```
config ips settings
      set ips-packet-quota <integer>
      set packet-log-history <integer>
      set packet-log-post-attack <integer>
end
```

### Using HA log messages to determine system status

When the FortiGate unit is in HA mode, you may see the following log message content within the event log:

```
type=event subtype=ha level=critical msg= "HA slave heartbeat interface internal lost
    neighbor information"
```

OR

```
type=event subtype=ha level=critical msg= "Virtual cluster 1 of group 0 detected new
    joined HA member"
```

OR

```
type=event subtype=ha level=critical msg= "HA master heartbeat interface internal get peer
    information"
```

The log messages occur within a given time, and indicate that the units within the cluster are not aware of each other anymore. These log messages provide the information you need to fix the problem.

# Connection issues between FortiGate unit and logging devices

If external logging devices are not recording the log information properly or at all, the problem will likely be due to one of two situations: no data is being received because the log device cannot be reached, or no data is being sent because the FortiGate unit is no longer logging properly.

## Unable to connect to a supported log device

After configuring logging to a supported log device, and testing the connection, you may find you cannot connect. To determine whether this is the problem:

1. Verify that the information you entered is correct; it could be a simple mistake within the IP address or you may have not selected **Apply** on the Log Settings page after changing them, which would prevent them from taking effect.
2. Use `execute ping` to see if you can ping to the log device.
3. If you are unable to ping to the log device, check to see if the log device itself working and that it is on the network and assigned an appropriate address.

## FortiGate unit has stopped logging

If the FortiGate unit stopped logging to a device, test the connection between both the FortiGate unit and device using the execute ping command. The log device may have been turned off, is upgrading to a new firmware version, or just not working properly.

The FortiGate unit may also have a corrupted log database. When you log into the web-based manager and you see an SQL database error message, it is because the SQL database has become corrupted. View "SQL database errors" in the next section before taking any further actions, to avoid losing your current logs.

# Log database issues

If attempting to troubleshoot issues with the SQL log database, use the following to help guide you to solving issues that occur.

## SQL statement syntax errors

There may be errors or inconsistencies in the SQL used to maintain the database. Here are some example error messages and possible causes:

```
You have an error in your SQL syntax (remote/MySQL)
```

or

```
ERROR: syntax error at or near... (local/PostgreSQL)
```

- Verify that the SQL keywords are spelled correctly, and that the query is well-formed.
- Table and column names are demarked by grave accent (`) characters. Single (') and double (") quotation marks will cause an error.

```
No data is covered.
```

- The query is correctly formed, but no data has been logged for the log type. Verify that you have configured the FortiGate unit to save that log type. On the Log Settings page, make sure that the log type is checked.

## Connection problems

If well-formed SQL queries do not produce results, and logging is turned on for the log type, there may be a database configuration problem with the remote database.

Ensure that:

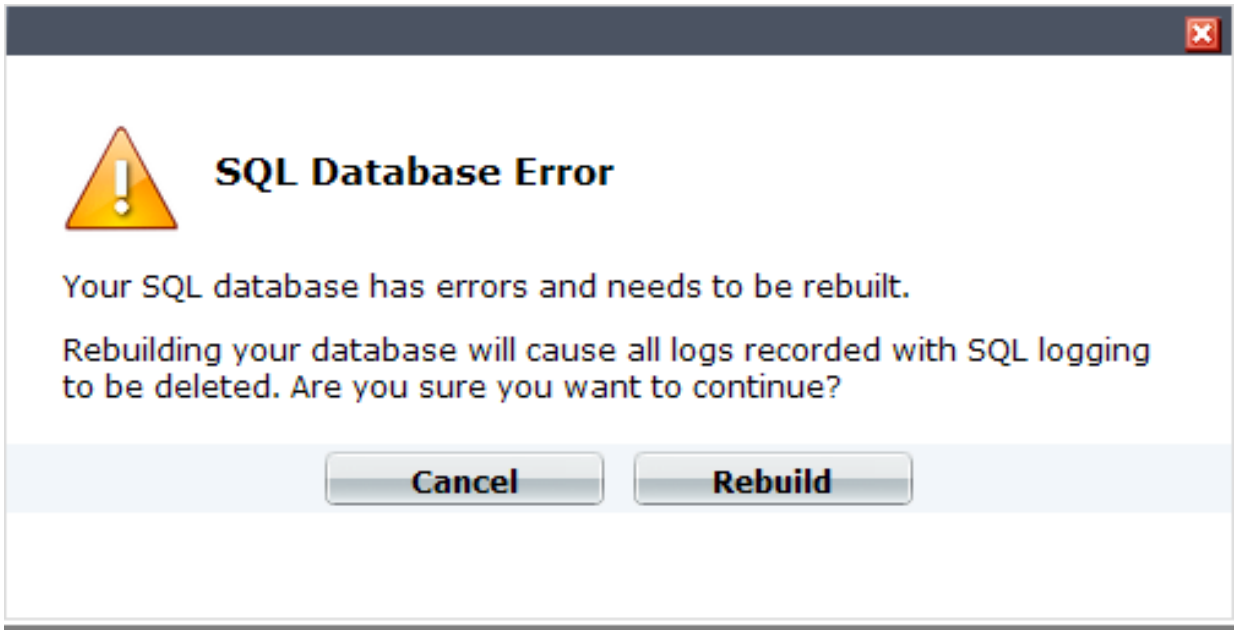
- MySQL is running and using the default port 3306.
- You have created an empty database and a user who has read/write permissions for the database.
- Here is an example of creating a new MySQL database named fazlogs, and adding a user for the database:

1. `#Mysql –u root –p`
2. `mysql>` Create database fazlogs;
3. `mysql>` Grant all privileges on fazlogs.* to ‘fazlogger’@’*’ identified by ‘fazpassword’;
4. `mysql>` Grant all privileges on fazlogs.* to ‘fazlogger’@’localhost’ identified by ‘fazpassword’;

## SQL database errors

If the database seems inacessible, you may encounter the following error message after upgrading or downgrading the FortiGate unit’s firmware image.

**Example of an SQL database error message**




The error message indicates that the SQL database is corrupted and cannot be updated with the SQL schemas any more. When you see this error message, you can do one of the following:

- select **Cancel** and back up all log files; then select **Rebuild** to blank and rebuild the database.
- select **Rebuild** immediately, which will blank the database and previous logs will be lost.

Until the database is rebuilt, no information will be logged by the FortiGate unit regardless of the log settings that are configured on the unit. When you select **Rebuild**, all logs are lost because the SQL database is erased and then rebuilt again. Logging resumes automatically according to your settings after the SQL database is rebuilt.

To view the status of the database, use the `diagnose debug sqldb-error status` command in the CLI. This command will inform you whether the database has errors present.

If you want to view the database's errors, use the `diagnose debug sqldb-error read` command in the CLI. This command indicates exactly what errors occurred, and what tables contain those errors.

Log files are backed up using the `execute backup {disk | memory } {alllogs | logs}` command in the CLI. You must use the text variable when backing up log files because the text variable allows you to view the log files outside the FortiGate unit. When you back up log files, you are really just copying the log files from the database to a specified location, such as a TFTP server.

## Logging daemon (Miglogd)

The number of logging daemon child processes has been made available for editing. A higher number can affect performance, and a lower number can affect log processing time, although no logs will be dropped or lost if the number is decreased.

If you are suffering from performance issues, you can alter the number of logging daemon child processes, from 0 to 15, using the following syntax. The default is 8.

```
config system global
   set miglogd-children <integer>
end
```